WHAT IS CLAIMED IS:

1. In a wireless LAN (WLAN) having an interworking function, a method for interworking between the WLAN and a second network, the WLAN and the second network capable of communicating with a broker entity, the method comprising the steps of:

receiving from the broker, a first key;

receiving from a user device, a second network to user certificate that includes a broker to second network certificate and a second key;

authenticating the broker to second network certificate using the first key to derive a third key;

authenticating the second network to user certificate using the third key to derive the second key;

generating a session key, encrypting the session key using the second key, and transmitting the encrypted session key to the user device; and

communicating with the user device using the session key.

2. The method of claim 1, wherein the second network to user certificate further includes a subscription level of the user that indicates whether the user is subscribed for an interworking service, and the generating step is performed in response to the subscription level.

3. The method of claim 1, wherein the second network to user certificate further includes an expiration time of the second network to user certificate, and the method further comprises the step of checking the expiration time to determine whether the second network to user certificate has expired.

4. The method of claim 1, further including the step of generating a WLAN to user certificate that is signed with a fifth key and includes the session key, whereby the user device is able to authenticate the WLAN.

5. In a wireless LAN (WLAN) having an interworking function, a method for interworking between the WLAN and a second network, the WLAN and the second network capable of communicating with a broker entity, the method comprising the

steps of:

receiving, from the broker, a broker public key;

receiving, from a user device, a second network to user certificate, which is signed with a second network private key and includes a broker to second network certificate and a user public key, the broker to second network certificate being signed with a broker private key and including a second network public key;

authenticating the broker to second network certificate using the broker public key and deriving the second network public key;

authenticating the second network to user certificate using the second network public key and deriving the user public key;

generating a session key, encrypting the session key using the user public key, and transmitting the encrypted session key to the user device; and

communicating with the user device using the session key.

6. The method of claim 5, wherein the second network to user certificate further includes a subscription level of the user that indicates whether the user is subscribed for an interworking service, and the generating step is performed in response to the subscription level.

7. The method of claim 5, wherein the second network to user certificate further includes an expiration time of the second network to user certificate, and the method further comprises the step of checking the expiration time to determine whether the second network to user certificate has expired.

8. The method of claim 5, further including the step of providing the user device with an ability to authenticate the WLAN.

9. The method of claim 8, wherein the providing step comprises the steps of:

receiving a broker to WLAN certificate signed with the broker private key and includes a WLAN private key;

generating a WLAN to user certificate that is signed with the WLAN private key and includes the encrypted session key; and

transmitting the WLAN to user certificate to the user device.

10. A method for communicating with a wireless LAN (WLAN) using a user device that has a subscription to a second network, the second network having an interworking contract with the WLAN, the WLAN and the second network capable of communicating with a broker entity, the method comprising the steps of:

receiving, from the second network, a second network to user device certificate, which is signed with a second network private key, and includes a broker to network certificate and a user public key;

transmitting to the WLAN the second network to user device certificate, wherein the WLAN is able to derive the user public key using a broker public key received from the broker entity;

receiving, from the WLAN, a session key encrypted using the user public key;

decrypting the session key with a user private key; and

communicating with the WLAN using the session key.

11. The method of claim 10, wherein the second network to user certificate further includes a subscription level of the user that indicates whether the user is subscribed for an interworking service.

12. The method of claim 10, wherein the second network to user certificate further includes an expiration time of the second network to user certificate, and the transmitting step is performed if the expiration time has not expired.

13. The method of claim 10, wherein the receiving step comprises receiving a WLAN to user certificate signed with the broker private key and including the session key, and further comprising the steps of receiving, from the second network, the broker public key, and authenticating the WLAN to user certificate using the broker public key and deriving the session key.

14. A broker based system for authenticating users in networks having interworking relationships, comprising:

a wireless LAN (WLAN) having an interworking function;

a second network; and

a broker entity capable of communicating with the WLAN and the second

network, the broker having means for transmitting a broker public key to the WLAN, and means for transmitting a broker to second network certificate, which is signed with a broker private key and includes a second network public key, to the second network,

the second network including means for transmitting, to a user device, a second network to user certificate signed with a second network private key and includes the broker to second network certificate and the user public key,

the WLAN including means for authenticating the broker to second network certificate and deriving the second network public key, means for authenticating the second network to user certificate and deriving the user public key, and means for generating a session key and encrypting the session key with the user public key.

15. The method of claim 14, wherein the WLAN further includes means for transmitting a WLAN to user certificate signed with a WLAN private key and includes the encrypted session key.